CLAIMS

What is claimed is:

1. A process for generating, delivery, and validation of electronic coupons via a telecommunication system, comprising the sub-processes of:

generating a coupon authentication number for each receiving device;

delivering a cryptographic electronic coupon to one or more receiving devices;

validating said cryptographic coupon when a user applies to redeem said cryptographic coupon;

wherein said telecommunication system includes a service center, a plurality of receiving devices, a display device coupled to each receiving device, a communication channel connecting said service center and each receiving device;

wherein said service center comprises an activation database, an authentication number database and a key server;

wherein said receiving device comprises a persistent storage device which stores one or more public keys assigned to said receiving device, and a crypto-chip which stores one or more private keys assigned to said receiving device; and

wherein said communication channel may be a telephone modem, a cable modem, or a local area network.

2. The process according to Claim 1, wherein the sub-process of generating a coupon authentication number for each receiving device comprises the steps of:

activating said receiving device;

generating a coupon authentication number for each said receiving device, wherein said coupon authentication number is randomly given and can be of any length of bits;

saving said authentication number in said authentication number database;

communicating said coupon authentication number to said key server;

encrypting said coupon authentication number; and

sending encrypted coupon authentication number to said receiving device which adds said encrypted authentication number to said receiving device's keyring as a coupon key.

3. The process according to Claim 2, wherein said step of encrypting said coupon authentication number is performed by said key server using said receiving device's El Gamal public key which is stored both in said activation database and said receiving device's persistent storing device.

4. The process according to Claim 2, further comprising the step of:

embedding a date or time stamp in said coupon key for convenience to replace said authentication number when ever said authentication number database is compromised.

5. The process according to Claim 1, wherein the sub-process of delivering cryptographic coupon to one or more receiving devices, comprising the steps of:

receiving an order from a client to issue an electronic coupon, which is an offer to sell a specific product or service;

confirming an offer ID number for said coupon;

sending said offer ID number with coupon information to said display device through said receiving device;

performing a hash operation by said crypto-chip on said offer ID number using said encrypted coupon authentication number if a user decides to accept said offer; and

displaying the first N digits of the hashed result as a coupon ID number, with which, together with said offer ID number and said receiving device's serial number, the user may redeem said coupon.

6. The process according to Claim 5, wherein said step of confirming a unique offer ID number for said coupon comprises the sub-steps of:

checking whether or not said client has designated a unique offer ID number for said coupon;

wherein if said client has designated a unique offer ID number for said coupon, checking the uniqueness of said offer ID number and resolving possible collisions with other offers; and

wherein if said client has not designated a unique offer ID number for said coupon, generating a unique offer ID number for said coupon.

7. The process according to Claim 5, wherein said offer ID number is implemented as ASCII character strings.

8. The process according to Claim 6, wherein N is 6.

9. The process according to Claim 1, wherein the sub-process of validating said cryptographic coupon comprises the steps of:

submitting said offer ID number, said receiving device's serial number, and said coupon ID number to a vendor by the user who accepted said coupon;

entering said offer ID number, said receiving device's serial number, and said coupon ID number by said vendor who accesses to a common gate interface at said service center;

checking, by said key server, the unencrypted authentication number from said coupon authentication number database;

performing a hash function on said offer ID number using said unencrypted authentication number as a key;

taking the first N digits of the hashed result and comparing this N-digit number with said coupon ID number submitted by the user; and

validating said coupon if said N-digit number match with said coupon ID number.

10. A method for generating a coupon authentication number for each receiving device coupled to a coupon distribution system, comprising the steps of:

activating said receiving device;

generating a coupon authentication number for each said receiving device, wherein said coupon authentication number is randomly given and can be of any length of bits long;

storing said coupon authentication number in said coupon authentication number database;

communicating said coupon authentication number to said key server;

encrypting said coupon authentication number; and

sending encrypted coupon authentication number to said receiving device which adds said encrypted coupon authentication number to said receiving device's keyring as a coupon key.

11. The method according to Claim 10, wherein said step of encrypting said coupon authentication number is performed by said key server using said receiving device's El Gamal public key which is stored both in said activation database and said receiving device's persistent storing drive.

12. The method according to Claim 10, further comprising the step of:

embedding a date or time stamp in said coupon key for convenience to replace said coupon authentication number when ever said authentication number database is compromised.

13. A method for delivering cryptographic coupon to one or more receiving devices coupled to a coupon distribution system, comprising the steps of:

receiving an order from a client to issue an electronic coupon, which is an offer to sell a specific product or service;

confirming an offer ID number for said coupon;

sending said offer ID number with coupon information to said display device through said receiving device;

performing a hash operation by said crypto-chip on said offer ID number using said encrypted coupon authentication number if a user decides to accept said offer;

displaying the first N digits of the hashed result as coupon ID number, with which, together with said offer ID number and said receiving device's serial number, the user may redeem said coupon; and

wherein said coupon ID number may be displayed by either a stopwatch icon or a screen including detailed instruction about how to redeem said coupon.

14. The method according to Claim 13, wherein said step of confirming a unique offer ID number for said coupon comprises the sub-steps of:

checking whether or not said client has designated a unique offer ID number for said coupon;

if yes, checking the uniqueness of said offer ID number and solving possible collisions with other offers;

if not, generating a unique offer ID number for said coupon; and

wherein said offer ID number may be any length of bits.

15. The method according to Claim 13, wherein said offer ID number is implemented as ASCII character strings.

16. The method according to Claim 13, wherein N is 6.

17. A method for validating said cryptographic coupon, comprising the steps of:

submitting said offer ID number, said receiving device's serial number, and said coupon ID number to a vendor by the user who accepted said coupon;

entering said offer ID number, said receiving device's serial number, and said coupon ID number by said vendor who accesses to a common gateway interface at said service center;

checking, by said key server, the unencrypted authentication number from said coupon authentication number database;

performing a hash operation on said offer ID number using said unencrypted authentication number as a key;

taking the first N digits of the hashed result and comparing this N-digit number with said coupon ID number submitted by the user; and

validating said coupon if said N-digit number matches with said coupon ID number.

18. A system for coupon encryption, distribution, and validation, comprising:

a client which issues coupons, each of said coupons is designated a unique offer ID number;

an information service center which comprises an activation database, a coupon authentication number database, and a key server;

a plurality of service receiving devices, each of which is coupled to a displaying device;

a channel through which said information service center and said service receiving device communicate;

wherein said information service center generates a coupon authentication number for each said service receiving device, wherein said coupon authentication number is stored in said coupon authentication number database and is communicated to said key server;

wherein said key server encrypts said coupon authentication number using El Gamal algorithm and sends encrypted authentication number to said service receiving device;

wherein said service receiving device comprises a crypto-chip and a hard drive;

wherein said crypto-chip performs a hash operation on said offer ID number using said encrypted coupon authentication number and takes the first or last N digits of the hashed result as a coupon ID number for said coupon; and

wherein said coupon may be validated by said key server, which uses said service receiving device's serial number to look up the unencrypted coupon authentication number stored in said coupon authentication number database and performs a hash operation on said offer ID number using said unencrypted coupon authentication number and compares a base number taken from the first or last N digits of the hashed result with said coupon ID number submitted, and validates said coupon if said base number and said coupon number match.

19. The system according to Claim 18, wherein said receiving device is a personal video recorder and said displaying device is a TV set.

20. The system according to Claim 18, wherein said channel is a telephone modem, or a cable modem, or a local area network.

21. The system according to Claim 18, wherein said coupon authentication number is randomly given and can be of any length of bits.

22. The system according to Claim 18, wherein said offer ID number is randomly given and can be of any length of bits.

23. The system according to Claim 18, wherein said offer ID number is implemented as ASCII character strings.

24. The system according to Claim 18, wherein N is 6.

25. A method for preventing security leak of authentication number database, comprising the steps of:

keeping said authentication number database behind a firewall; and

denying access of unauthorized machines.

26. A method for remedying security leak of authentication number database, comprising the steps of:

fixing said security leak;

generating a new random coupon authentication number for each said receiving device; and

distributing said coupon authentication number to said receiving device via said key server.